BLOOD HURST & O'REARDON, LLP
TIMOTHY G. BLOOD (149343)
PAULA R. BROWN (254142)
JAMES M. DAVIS (301636)
501 West Broadway, Suite 1490
San Diego, CA 92101
Tel: 619/338-1100
619/338-1101 (fax)
tblood@bholaw.com
toreardon@bholaw.com
jdavis@bholaw.com

EVANGELISTA WORLEY, LLC
James M. Evangelista (*pro hac vice forthcoming*)
500 Sugar Mill Road, Suite 245A
Atlanta, GA 30350
Tel: 404/205-8400
404/205-8395 (fax)
jim@ewlawllc.com

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA – SAN FRANCISCO DIVISION

JEAN-RÉMI MASSERY, individually and on behalf of all others similarly situated, Plaintiff, v. COINBASE GLOBAL, INC.; COINBASE, INC., Defendants.	Case No. 23-cv-04026 **CLASS ACTION COMPLAINT** **<u>CLASS ACTION</u>** **JURY TRIAL DEMANDED**

Plaintiff Jean-Rémi Massery files this Class Action Complaint against Coinbase Global, Inc. and Coinbase, Inc. (collectively, "Coinbase") for damages, injunctive relief, and other equitable relief. Plaintiff brings this action based upon personal knowledge of the facts pertaining to him, and on information and belief as to all other matters, by and through the investigation of undersigned counsel.

INTRODUCTION

1. This class action is on behalf of all European Union resident Coinbase "wallet" and account holders who have had their wallets or accounts hacked by third parties and/or frozen by Coinbase.

2. Coinbase is the largest cryptocurrency exchange in the United States. According to Coinbase, it has "built [its] reputation on the premise that [it] offers customers a secure way to purchase, store, and transact in crypto assets." In its words, what "sets [Coinbase] apart" from competitors is its "customer technology[,] [which is] built to deal with the real-time, global, and 24/7/365 nature of the crypto asset markets."

3. Yet Coinbase's wallet and account services were not "secure." As demonstrated by the widespread successful hacking and fraud perpetrated against Coinbase users, Coinbase lacked adequate security to prevent its users' funds from being drained by scammers and hackers; it lacked, or failed to follow, adequate policies, practices, and procedures to protect the safety and security of Plaintiff's and Class Members' assets; it lacked adequate warning and notification systems and processes to warn its customers of specific risks of theft and fraud associated with certain third party websites that Coinbase allowed its customers to unwittingly connect to, and it lacked adequate staffing to carry out its policies, practices, and procedures to the extent they were designed to protect its customers wallets and accounts.

4. Moreover, when Coinbase users reported fraudulent activity in their account (or simply at random in the absence of suspected fraud), Coinbase improperly and unreasonably locked out its consumers from accessing their accounts and funds, either for unnecessarily lengthy periods of time or even permanently. Because of the extreme volatility of cryptocurrencies' value – with freefalls of 40% within 24 hours not unheard of – the inability to access an account to sell, buy, or

trade cryptocurrency leads to severe financial loss. Making matters worse, Coinbase failed to timely respond to customer pleas for support and help, and also failed to preserve and safeguard customer funds as it promises. Coinbase's failures have prevented Plaintiff and Class Members from having "full control of your crypto" and from being able to "invest, spend, save, earn, and use," or withdraw their funds as Coinbase promises.

5. As a result of Coinbase's conduct, Plaintiff and Class Members have been damaged through the theft of their funds and investments in their Coinbase wallets and accounts, lost investment opportunities, and the fees they paid to Coinbase for the fraudulent transactions in their wallets and accounts. Accordingly, Plaintiff seeks damages and equitable relief on behalf of themselves and those similarly situated.

THE PARTIES

6. Plaintiff Jean-Rémi Massery is a resident of France. Relying on Coinbase's representations about the security of an account and wallet, his funds, and his cryptocurrency, Plaintiff Massery opened an account and a wallet with Coinbase through which he deposited funds and traded cryptocurrency. Consistent with Coinbase's representations, Plaintiff Massery had a reasonable expectation that his funds and cryptocurrency would be safe, that he would be able to access his account and wallet whenever he wanted, that he could utilize the wallet platform without fear of fraud, and that his funds and cryptocurrency would not be stolen. Mr. Massery's wallet and account, however, were accessed by an unauthorized third party, and his funds and cryptocurrency were stolen. As a result of Defendants' acts and inaction, Plaintiff Massery and the similarly situated putative class members he seeks to represent have suffered injury in fact and lost money or property when their funds and cryptocurrency were stolen.

7. Defendant Coinbase Global, Inc. is a publicly traded Delaware company that is involved in the business of cryptocurrency exchange, among other interrelated businesses. Defendant Coinbase Global operates worldwide on a virtual platform and claims not to have a formal physical headquarters since it is a "remote first" company. Coinbase Global in fact currently maintains its executive offices in San Francisco, California, and maintained such offices at times

relevant to this litigation. Among its subsidiaries, Coinbase Global owns defendant Coinbase, Inc. and Coinbase Custody Trust Company, LLC.

8. Defendant Coinbase, Inc., a California company, is a wholly owned subsidiary of Coinbase Global, Inc. Defendant Coinbase, Inc. also currently maintains its executive offices in San Francisco, California, and maintained such offices at times relevant to this litigation. Among its subsidiaries, Coinbase, Inc. owns and operates Toshi Holdings Pte Ltd (d/b/a Coinbase Wallet). Coinbase owns the cryptocurrency trading platform and was licensed in January 2017 by the New York State Department of Finance to operate both a virtual currency business, through a BitLicense (or the Department's Limited Purpose Trust Charter) and money transmitter business in the State of New York. As a condition of its licenses, Coinbase, Inc. was required to comply with a variety of New York laws and regulations governing virtual currency companies, money transmitters and cybersecurity including, for example:

- Section 200.15(h) of Title 23 of the New York Codes, Rules, and Regulations requiring virtual currency licensees to maintain a customer identification program, and must, at a minimum, verify the customer's identity, to the extent reasonable and practicable, maintain records of the information used to verify such identity, including name, physical address, and other identifying information;

- Section 200.15(e)(3) further requires that licensees shall monitor for transactions that might signify money laundering, tax evasion, or other illegal or criminal activity and shall file Suspicious Activity Reports ("SARs") in accordance with applicable federal laws, rules, and regulations;

- Section 200.15(b) also requires that licensees shall conduct an initial risk assessment that will consider legal, compliance, financial, and reputational risks associated with the licensee's activities, services, customers, counterparties, and geographic location;

- Section 417.2(a) of Title 3 of the New York Codes, Rules, and Regulations also requires money transmitter licensees to incorporate policies, procedures, and internal controls reasonably designed to assure compliance application Federal law including verifying customer identification, filing reports; creating and retaining records; and

- Section 500.17 of the Superintendent's Regulations requires that each covered entity shall notify the Department as promptly as possible but in no event later than 72 hours from a determination that a cybersecurity event has occurred where either notice is required to be provided to any government body, self-regulatory agency or any other supervisory body, or where the event has a reasonable likelihood of materially harming any material part of the normal operation(s) of the covered entity.

9. Through operating a cryptocurrency exchange, Coinbase is and was at all relevant times a “money transmitter” as defined by the Bank Secrecy Act and its implementing regulations. As such, Coinbase is and was at all relevant times required to comply with BSA regulations applicable to money services businesses, including strict compliance obligations under the BSA to monitor customer transactions and report any suspicious activities to law enforcement authorities. *See generally* 31 C.F.R. § 1022 (Rules for Money Services Businesses).

10. Coinbase is and at all relevant times was a “financial institution” with compliance obligations under the Electronic Funds Transfer Act, 15 U.S.C. § 1693, *et seq.*, including the EFTA’s error resolution provisions, 15 U.S.C. § 1693f.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount-in-controversy, exclusive of costs and interests, exceeds the sum of $5,000,000.00, in the aggregate, as there are well over 100 members of the Class who are known to exist, and this is a class action in which Plaintiff is from a different country than the Defendants. Moreover, the Coinbase Wallet Terms of Service agreements Plaintiff and putative Class Members signed when they opened their Coinbase accounts and wallets provided for the exclusive jurisdiction of all disputes in the Northern District of California and pursuant to California law without regard to its conflict of law provisions.

12. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b). Defendants reside in this district, their principal executive office is located here, a substantial part of the events or omissions giving rise to the claims occurred here and/or a substantial part of property that is the subject of the action is situated here.

13. Assignment is proper to the San Francisco Division of the Northern District of California under Civil L.R. 3-2(c) and (d) because a substantial part of the events or omissions that gave rise to Plaintiff’s claims occurred in San Francisco County and because the Coinbase Wallet Terms of Service Plaintiff and putative class members signed when they opened their Coinbase accounts and wallets provided for the exclusive jurisdiction of all disputes in the Northern District of California.

FACTUAL ALLEGATIONS

Background

14. Coinbase is an online exchange platform for cryptocurrency transactions. It currently boasts $145 billion in crypto assets traded quarterly, $130 billion in assets maintained on its platform, and approximately 98 million customers located in over 100 countries that trade in custodial fiat currencies and cryptocurrencies.

15. Coinbase holds itself out as providing the primary financial account for the crypto economy – a safe, trusted, and easy-to-use platform to invest, store, spend, earn, and use crypto assets. For example, Coinbase stated it is "the easiest place to buy and sell cryptocurrency" and is "The most trusted cryptocurrency platform."[1] Likewise, Coinbase represented on its website—as the reason to use its hosted wallet service—that customers are able to be "in full control of your crypto" and that its hosted wallet "is the easiest solution" for users to "buy, sell, send and receive crypto."[2] It also represented that it offers "a more fair, accessible, efficient, and transparent financial system enabled by crypto."[3] Coinbase claimed on its website that, as part of its "Security for Your Peace of Mind," it undertakes "careful measures to ensure that [Coinbase users'] bitcoin is as safe as possible" and that "98% of customer funds are stored offline."[4] Coinbase further claimed that it followed "industry best practices" regarding account security.[5]

16. Plaintiff and the other members of the Class reasonably believed that Coinbase would provide the safe, secure, and easy-to-access platform it promised.

17. Plaintiff, like the other Class Members he seeks to represent, opened wallets (accounts) hosted by Coinbase that purportedly enable him to conduct transactions in cryptocurrency 24 hours a day, 7 days a week and 365 days a year. Each Coinbase customer's account and wallet reflects those transactions and permits access to their cash, crypto assets (*e.g.*, cryptocurrencies) and other investment funds. Accordingly, Plaintiff, and each wallet or account

[1] https://www.coinbase.com/
[2] https://www.coinbase.com/learn/tips-and-tutorials/how-to-set-up-a-crypto-wallet
[3] https://www.coinbase.com/about
[4] https://www.coinbase.com/security
[5] https://www.coinbase.com/

holder, are entitled to, reasonably expect, and must have access to their accounts, wallets and the funds and cryptocurrencies held therein at all times.

18. Coinbase operates an online cryptocurrency trading platform on which its account and wallet holder customers can buy, sell, spend, and trade cryptocurrency, such as Bitcoin, Ethereum, and Litecoin. Coinbase's platform also facilitates access to account holders' cryptocurrencies and funds through a digital "wallet," including customer proceeds for the purchase, and from the sale, of cryptocurrencies.

19. Coinbase represented to its customers that it is a fully compliant, regulated entity, registered as a Money Services Business with FinCEN, the United States Department of the Treasury's Financial Crimes Enforcement Network.

20. Coinbase earned the vast majority of its revenue, approximately $3 billion in 2022, through fees generated from its individual customers' retail trade transactions in cryptocurrency. It also earns money on funds held in customer accounts through its deposits and investments.

21. Coinbase recognized the responsibilities, risks, and liabilities it undertakes holding Plaintiff's, Class Members' and its other customers' valuable financial assets. For example, Coinbase made the following statement in its Supplement No. 1 to its April 1, 2021, prospectus filed with the Securities and Exchange Commission:

> The Company has committed to securely store all crypto assets it holds on behalf of users. As such, the Company may be liable to its users for losses arising from theft or loss of user private keys.

In connection with that representation, Coinbase indicated that "it accounts for and continually verifies the amount of crypto assets within its control, and … has established security around custodial private keys to minimize the risk of theft or loss."

22. Coinbase also made the following statement in its Supplement No.1: "Our business involves the collection, storage, processing, and transmission of confidential information, customer, employee, service provider, and other personal data, as well as information required to access customer assets. We have built our reputation on the premise that our platform offers customers a secure way to purchase, store, and transact in crypto assets.

23. Coinbase represented that its security measures "will provide absolute security or prevent breaches and attacks," and "we have developed systems and processes designed to protect the data we manage, prevent data loss and other security breaches, effectively respond to known and potential risks, and expect to continue to expend significant resources to bolster these protections…."

24. Based at least in part on its representations about the safety of its customers' transactions, and assets held in customer accounts and wallets, Coinbase experienced tremendous growth. For example, Coinbase verified users grew from a total of approximately 13 million in September 2017 to approximately 98 million as of the end of 2022. Similarly, Coinbase grew from only 199 employees at the end of 2017 to 1,717 employees as of March 31, 2021, approximately 40% of which then worked in engineering, product and design teams. Coinbase represents on its website that it has over 3,500 employees today, nearly doubling over the last two years, many of which presumably were hired as a result of facts at issue in this litigation, among other lawsuits and investigations.

25. Coinbase users, such as Plaintiff and Class Members, are subject to the Coinbase Wallet Terms of Service in effect when they opened their account and wallet with Coinbase.

26. However, as residents of members states of the European Union, Plaintiff and Class Members are not subject to any arbitration provision because such provisions in consumer agreements are not enforceable throughout the European Union and Coinbase's Terms of Service do not contain one.

27. Moreover, the Terms of Service provided that all disputes "will be governed by the laws of the state of California in the United States, without regard to its conflict of laws provisions" and that all disputes will be resolved "exclusively in the state courts located in the City and County of San Francisco, California, or federal court for the Northern District of California."

28. Coinbase knew, or should have known, that when Plaintiff and Class Members opened their accounts and wallets, and placed their financial and crypto assets into those accounts and wallets, Coinbase would not be able to provide adequate security to prevent Plaintiff's and Class Members' accounts from being hacked or hijacked by fraudulent third parties and their assets stolen.

29. Coinbase knew, or should have known, that when Plaintiff and Class Members opened their accounts and wallets, Coinbase did not have adequate policies, practices and procedures in place to protect the safety and security of Plaintiff's and Class Members' assets.

30. Coinbase knew, or should have known, that when Plaintiff and Class Members opened their accounts and wallets, Coinbase did not have adequate staffing in place to protect the safety and security of Plaintiff's and Class Members' assets.

31. Accordingly, at the time when Plaintiff and Class Members opened their accounts and wallets, Coinbase misrepresented to Plaintiff and Class Members that their assets in trust with Coinbase were safe and secure.

New York State Dept. of Financial Services Issues Consent Order Against Coinbase

32. Beginning in May 2020, the New York State Department of Financial Services (the "Department") conducted a supervisory examination for the time period July 1, 2018, through December 31, 2019 (the "Examination") of Coinbase's compliance function across multiple areas. The Department's Report of Examination, detailing the results of that examination, was transmitted to Coinbase's leadership in September 2020, and found that "Coinbase's compliance system failed to keep up with the dramatic and unexpected growth of Coinbase's business, and, by the end of 2021, was overwhelmed with a substantial backlog of unreviewed transaction monitoring alerts, exposing its platform to risk of exploitation by criminals and other bad actors."

33. Among other things, the Department's Examination found significant deficiencies across Coinbase's compliance program, including its Know-Your-Customer/Customer Due Diligence ("KYC/CDD") procedures, its Transaction Monitoring System ("TMS"), and its Office of Foreign Assets Control screening program ("OFAC"), and that Coinbase had not provided evidence of a validation review of its TMS system, as required by 23 NYCRR 504.3(a). The Department's investigation further uncovered substantial lapses in Coinbase's KYC/CDD program and its TMS, as well as issues concerning Coinbase's retention of books and records.

34. According to the Department:

> Over the course of 2021, it became clear that Coinbase's compliance system was inadequate to handle the growing volume of Coinbase's business, a situation that was exacerbated by tremendous growth in its customer base....

> Indeed, during the course of the Department's investigation, the compliance situation inside Coinbase reached a critical stage. By the end of 2021, Coinbase had a backlog of unreviewed transaction monitoring alerts grew to more than 100,000 (many of which were months old), and the backlog of customers requiring enhanced due diligence ("EDD") exceeded 14,000.
>
> These backlogs were exacerbated by business and operational growth occurring in 2020 through 2021. For example, Coinbase customer sign ups in May 2021 were fifteen times January 2020 levels, and monthly transactions in November 2021 were twenty-five times January 2020 levels.
>
> At that time, Coinbase lacked sufficient personnel, resources, and tools needed to keep up with these alerts, and backlogs rapidly grew to unmanageable levels. This was compounded by Coinbase's reliance in 2019 through November 2021 on an inadequate case management system for dispositioning alerts and filing.

January 4, 2023, Consent Order between Coinbase and the Department (the "Consent Order").[6]

35. As further found in the Consent Order:

- The most serious noncompliance concerns Coinbase's ML/TF compliance program, specifically in its customer onboarding and transaction monitoring obligations. Coinbase has acknowledged its failures in this respect to the Department. Furthermore, certain of these issues have been known to Coinbase since at least 2018, flagged through both internal assessments and external reviews, including examinations conducted by the Department.

- The foundation of an adequate ML/TF compliance system is the maintenance of robust KYC/CDD policies, procedures, and processes tailored to the specific risks posed by the entity's business activities. KYC/CDD requirements protect financial systems by ensuring that financial services providers truly "know" their customers by understanding the nature and purpose of the customer's business, the source of the customer's funds, and the customer's true identity or ownership.

- During much of the relevant period, Coinbase's KYC/CDD program, both as written and as implemented, was immature and inadequate. Coinbase treated customer onboarding requirements as a simple check-the-box exercise and failed to conduct appropriate due diligence. Examples of Coinbase's customer due diligence failures during much of this timeframe include:

  a. Prior to December 2020, Coinbase often failed to assign an informed "risk rating" to individual retail customers at the time of onboarding, and no quality assurance process was in place concerning risk rating until September 2021;

  b. Coinbase's customer due diligence file from its retail customers historically consisted of little more than a copy of a photo ID;

[6] *In the Matter of: Coinbase, Inc.*, Consent Order (January 2023), available at https://www.dfs.ny.gov/system/files/documents/2023/01/ea20230104_coinbase.pdf.

> c. Coinbase historically did the bare minimum to verify customer due diligence information for customers, relying on self-reported social media profiles while overlooking information that was, on its face, clearly inaccurate, and/or incomplete;
>
> d. Prior to July 2021, Coinbase allowed customers to open accounts without supplying essential information such as annual expected activity, and account purpose;

> - Coinbase's lack of knowledge about its customers exposed the Company and the financial system to increased ML/TF risk. Appropriately, Coinbase's compliance program is "risk-based," that is, the amount of scrutiny an account or transaction is given depends upon the risk rating assigned to the account. Such a risk-based system, however, is only effective if the risk rating is conducted rationally, and that simply did not happen at Coinbase (and in many cases still has not happened) for accounts opened prior to December 2020.
>
> - Another bedrock ML/TF requirement is the maintenance of a transaction monitoring system ("TMS") sufficient to monitor customers' transactions, and to track, timely investigate, and appropriately address, any suspicious activity occurring on the institution's platform. Pursuant to Part 504 of the Superintendent's Regulations, Department licensees are required to have a system in place for monitoring transactions after their execution for potential ML/TF violations and suspicious activity reporting.
>
> - Generally, transaction monitoring systems are programmed to trigger an alert on certain elements of potentially suspicious transactions, which are then reviewed by specially trained compliance professionals who analyze the transaction involved in the alert. For example, TMS systems are commonly programmed to alert compliance personnel when a customer who normally transacts in low quantities suddenly begins transacting in much higher quantities. Other relevant factors include risk ratings, which in turn could impact certain triggering "thresholds" of the system. . . .
>
> - As previously discussed, Coinbase's business and customer base have grown exponentially since it was licensed by the Department, but Coinbase was unable to keep pace with the growth in the volume of alerts generated by its TMS. By late 2021, Coinbase's failure to keep pace with its alerts resulted in a significant and growing backlog of over 100,000 unreviewed transaction monitoring alerts.
>
> - The TMS alert backlog was caused, in substantial part, by Coinbase's inability to predict or manage the growing alert volume and a lack of adequate compliance staff.
>
> - Coinbase's efforts to remediate this backlog encountered numerous challenges.... Coinbase provided insufficient oversight over the third-party contractors it hired, and a substantial portion of the alerts reviewed by third parties was rife with errors.
>
> - Because the TMS deficiencies prevented Coinbase from properly monitoring the activity of its customers, Coinbase faced an increased risk of abuse by bad actors....

- As with the customer due diligence deficiencies, this risk is not merely theoretical. Although the full extent of activity that was contained in Coinbase's TMS backlog has not been fully determined, the Department has identified troubling examples of suspicious conduct that should have been identified, stopped, and (in some instances) reported to authorities but was not, at least initially, due to the backlog....

- One of the primary reasons for requiring a TMS is so that a financial institution can identify and prevent future suspicious transactions so that bad actors are not allowed to use a financial institution to facilitate illegal activity. Simply put, because of the backlogs, Coinbase's TMS system failed to sufficiently accomplish that goal.

- Financial institutions have the obligation to timely investigate and report to the Federal government any suspicious activity in the form of a SAR within 30 days of detection. Another consequence of Coinbase's failed TMS discussed above is that, as uninvestigated TMS alerts languished for months in the backlog, Coinbase routinely failed to timely investigate and report suspicious activity as required by law.

- The Department's investigation found numerous examples of SARs filed months, some more than six months, after the suspicious activity was first known to Coinbase.

- Furthermore, the Department found that Coinbase's record keeping of suspicious activity investigations and reporting was insufficient. For example, Coinbase was unable to meaningfully respond to the Department's request for data related to suspicious activity identification, tracking, and reporting that took place in 2018 and 2019 because it did not adequately track or retain that information.

- Coinbase allows its users to access its sites while using Virtual Private Networks ("VPNs") or The Onion Router ("TOR"). VPNs are a means of using a proxy web address as an interface between a user and a website. TOR disseminates web traffic across a distributed and anonymous network, such that the exit nodes for the network appear to be the user's web address. Both methods allow a user to appear to be located in a jurisdiction other than that of the user's actual, physical location.

- Notably, Coinbase has never promulgated a risk-based policy (for instance, instituting a rule that use of such tools raises the level of risk from medium to high, or from low to medium) for those users it detects using such tools. Instead, Coinbase allows its investigators to consider such activity as a factor in investigations.

- In sum, Coinbase knows there is technology widely available to circumvent geographic restrictions, knows that some of its customers use that technology, and has not structured its compliance program to fully account for the use of that technology, even if Coinbase does include certain mitigating controls addressing VPNs.

- In 2021 approximately 6,000 Coinbase customers appear to have been the victims of a phishing scam unrelated to Coinbase that ultimately led to unauthorized access of those customers' Coinbase accounts. Approximately $1.5 million was stolen from Coinbase's New York customers. Coinbase also reimbursed all customers who lost funds and worked closely with law enforcement to help hold accountable those who orchestrated this scam.

- However, although Coinbase was required by 23 NYCRR § 500.17 to report this event to the Department within 72 hours of its being discovered (and indeed reported the same event to the United States Secret Service on May 19, 2021), Coinbase did not report this event to the Department until September 17, 2021, five months after the event occurred. Coinbase has since updated its internal procedures to ensure timely notification of incidents are made to the Department.

- Coinbase conducted business in an unsafe and unsound manner, in violation of New York Banking Law § 44.

See Consent Order.

36. Pursuant to the Consent Order, Coinbase agreed to adopt a remediation plan to enhance its compliance program, agreed to pay a $50 million civil monetary penalty, agreed to retain an Independent Monitor to review Coinbase's compliance shortcomings and to assist the company to address those shortcomings," and agreed to "spend no less than fifty million U.S. dollars ($50,000,000.00) on further improvements and enhancements to its compliance program."

Coinbase's BSA/AML Obligations

37. Through operating as a cryptocurrency exchange, Coinbase is a "money transmitter" as defined by the Bank Secrecy Act ("BSA") and its implementing regulations. *See* 31 C.F.R. § 1010.100(ff). As such, Coinbase is required to comply with BSA regulations applicable to money services businesses. *See generally* 31 C.F.R. § 1022 (Rules for Money Services Businesses).

38. As a money services business, Coinbase has strict compliance obligations under the BSA to monitor customer transactions and report any suspicious activities to law enforcement authorities. *See* 31 U.S.C. § 5311; 31 U.S.C. § 1010.100(ff)(5).

39. Coinbase is required to "develop, implement, and maintain an effective anti-money laundering program." 31 C.F.R § 1022.210(a).

40. Coinbase's anti-money laundering program ("AML") must be "commensurate with the risks posed by the location and size of, and the nature and volume of the financial services provided by, the money services business." 31 C.F.R § 1022.210(b).

41. Coinbase's AML program must "be in writing" and "available for inspection to the Department of the Treasury upon request." 31 C.F.R § 1022.210(c).

42. Coinbase's anti-money laundering program must meet minimum requirements, including:

- Incorporate policies, procedures, and internal controls reasonably designed to assure compliance with this chapter.[7]
    - Those policies, procedures, and internal controls developed under 31 C.F.R. § 1022.210 must have provisions for complying with this chapter including…"(A) Verifying customer identification…; (B) Filing Reports; (C) Creating and retaining records; and (D) Responding to law enforcement requests."
- Designate a person to assure day to day compliance with the program and this chapter.
- Provide education and/or training of appropriate personnel concerning their responsibilities under the program, including training in the detection of suspicious transactions to the extent that the money services business is required to report such transactions under this chapter.
- Provide for independent review to monitor and maintain an adequate program.

31 C.F.R § 1022.210(d).

43. As is clear from the Consent Order, described *supra*, Coinbase failed to comply with laws and regulations concerning its BSA and AML obligations.

Coinbase's Electronic Funds Transfer Act (EFTA) Obligations

44. The EFTA and its corresponding regulations implemented by the Consumer Financial Protection Bureau ("CFPB"), 12 C.F.R. § 1005.1, *et seq*., were designed with the "primary objective" of "the provision of individual consumer rights. 15 U.S.C. § 1693; 12 C.F.R. § 1005.1(b).

45. Coinbase is a "financial institution" under the EFTA, which includes banks, credit unions, but also "any other person who, directly or indirectly, holds an account belonging to a consumer." 15 U.S.C. § 1693a(9). A "person" includes "a natural person or an organization, including a corporation…" 12 C.F.R. § 1005.2(j).

[7] "Chapter" refers to 31 C.F.R., Subtitle B, Chapter X (Financial Crimes Enforcement Network, Department of the Treasury).

46. An "account" includes any consumer asset account held directly or indirectly by a financial institution and established primarily for personal, family, or household purposes. 15 U.S.C. § 1693a(2); *see also* 12 C.F.R. § 1005.2(j).

47. A "consumer" is defined as a "natural person." 15 U.S.C. § 1693a(6).

48. An "error" includes, *inter alia*, an "unauthorized electronic fund transfer." 15 § 1693f(f)(1); 12 C.F.R. § 1005.11(a)(vii).

49. An "unauthorized electronic fund transfer" is defined as "an electronic fund transfer from a consumer's account initiated by a person other than the consumer without actual authority to initiate such transfer and from which the consumer receives no benefit." 15 U.S.C. § 1693(a)(12); see also 15 C.F.R. § 1005(m). The CFPB (as well as the Board of Governors of the Federal Reserve System) have specifically stated that "[a]n unauthorized [electronic funds transfer] includes a transfer initiated by a person who obtained the access device from the consumer through fraud or robbery." *See* 12 C.F.R. § 205, Supp. I at 2(m) (Board of Governors' Official Interpretation of § 205.2(m)); 12 C.F.R. § 1005, Supp. I at 2(m) (CFPB's Official Interpretation of § 1005.2(m)); *see also Green v. Capital One, N.A.*, 557 F.Supp.3d 441, 447 (S.D.N.Y. 2021).

50. An "electronic fund transfer" includes any transfer of funds initiated through a computer. While the definition does not include any transfer of funds the primary purpose of which is the purchase or sale of a security or commodity, if the security or commodity is regulated by the Securities and Exchange Commission ("SEC") or the Commodity Futures Trading Commission ("CFTC") or is purchased or sole through a broker-dealer regulated by the SEC or through a future commission merchant regulated by the CFTC, the "primary purpose" of the transfers of funds at issue in this action is not the purchase or sale of a security or commodity, but rather outright theft. The CFPB has made clear that this "Securities Exemption" applies to, for example, a transfer initiated by a telephone order to a stockbroker to buy or sell securities or to exercise a margin call, but not a transfer involving an access device that accesses a securities or commodities account that a consumer uses for purchasing goods or services or for obtaining cash (*i.e.*, a Coinbase account). 12 C.F.R. § 1005, Supp. I at 3(c)(4).

51. The error resolution subpart of the EFTA provides, in relevant part, that if a financial institution, within sixty days after having transmitted to a consumer notice of an electronic funds transfer, receives oral or written notice in which the consumer (1) sets forth or otherwise enables the financial institution to identify the name and account number of the consumer; (2) indicates the consumer's belief that the documentation, contains an error and the amount of such error; and (3) sets forth the reasons for the consumer's belief that an error has occurred, the financial institution must investigate the alleged error, determine whether an error has occurred, and report or mail the results of such investigation and determination to the consumer within ten business days. 15 U.S. Code § 1693f(a)(3); *see also* 12 C.F.R § 205.11; *see also* Supp. I to § 205 at 11(b)(1) (a notice of error is effective so long as the financial institution is able to identify the account in question); 12 C.F.R. § 1005, Supp. I at 11(b)(1)(1) (same). Notice may be constructive "when the institution becomes aware of circumstances leading to the reasonable belief that an unauthorized transfer to or from the consumer's account has been or may be made." 12 C.F.R. § 1005.6(b)(5)(iii).

52. If the financial institution determines that an error did occur, it has the option to either (1) timely correct the error, including the crediting of interest where applicable; or (2) timely provisionally recredit the consumer's account for the amount alleged to be in error pending the conclusion of the institution's investigation of the error within ten business days of being notified of the error. 15 U.S.C. § 1693f(c); *see also* 12 C.F.R. § 1005.11. In no circumstance can an investigation be concluded more than forty-five days after receipt of the notice of error, and during the pendency of the investigation, the consumer must be allowed full use of funds provisionally recredited. *Id*.

53. Where a financial institution (1) fails to provisionally recredit a consumer's account within the ten-day period specified above, and the financial institution (a) did not make a good faith investigation of the alleged error, or (b) did not have a reasonable basis for believing that the consumer's account was not in error; or (2) knowingly and willfully concludes that a consumer's account was not in error when such conclusion could not reasonably have been drawn from the evidence available to the financial institution at the time of its investigation, then the consumer shall be entitled to treble damages determined under section 1693m(a)(1).

54. As described herein, the electronic fund transfers at issue have been "unauthorized electronic fund transfers" because they have been initiated by either (i) an unauthorized person without actual authority to initiate such transfers or (ii) by a third person who fraudulently obtained authorization by Class Members, and from which Class Members have received no benefit. The primary purpose of such transfers have not been the purchase or sale of a security or commodity, but rather for the purpose of stealing Class Members' securities or commodities.

55. Plaintiff and Class Members provided timely actual and/or constructive notice to Coinbase of the unauthorized electronic transfers from their accounts. Indeed, Coinbase knew or should have known of the repeated and widespread breaches of its security and subsequent theft of customer funds and cryptocurrencies through a wide variety of readily identifiable, high volume, scamming operations, as well as repeated and widespread notifications to Coinbase from numerous Class Members of wallet and account thefts, fraud and scamming operations, such that it should have been aware of the need to implement adequate security and notification measures and monitor users' wallets and accounts for the additional of links to known scamming operations.

56. Coinbase failed to timely and in good faith investigate the unauthorized electronic transfers from Class Members' accounts as required by 15 U.S.C. § 1693f(a)(3) and 15 U.S.C. § 1693f(d) by failing to conduct a timely and reasonable review of its own records. *See* 12 C.F.R. § 205.11(c)(4); *see also* Supp. I to § 205 at 11(c)(4)–5. Adequate and timely investigations would have easily led Coinbase to the conclusion that widespread fraud had occurred, and was continually occurring, given that Class Members had either not authorized the transfers at issue or had granted access to their wallets and accounts to third party scamming operations, and that large numbers of Coinbase's customers had complained of unauthorized transfers in their accounts or wallets or that their accounts and wallets had been utilized by scammers to seal customer funds and Crypto assets such that Coinbase had locked those accounts, preventing customer access to them.

57. Further, Coinbase failed to timely correct the "errors" (as noted above, statutorily defined to include "unauthorized electronic fund transfers") when notified of them, or to correct the "errors" at all, in Class Members' accounts by timely crediting or provisionally recrediting Class

Members' accounts, or crediting or provisionally recrediting Class Members' accounts at all, after they had been breached and drained of funds. 15 U.S.C. § 1693f(b)-(c).

Plaintiff's Coinbase Transactions

58. Assured by Coinbase's representations of safety and security regarding his assets and transactions, Plaintiff Massery opened his account with Coinbase in late April or early May of 2020. The account was subject to Coinbase's Terms of Service.

59. After opening his account, Plaintiff Massery deposited personal funds into his account and began making crypto currency transactions. On or about August 10, 2021, an unauthorized person hacked his Coinbase wallet account, sold his crypto currency, opened a credit card, and removed all of his cash, for a loss totaling approximately €11,000 (Euro). Plaintiff Massery notified Coinbase by email on August 12, 2021, identified his account, his belief that the transactions at issue were fraudulent and the reasons for that belief, and the amounts and dates of the fraudulent transactions. Plaintiff Massery was immediately locked out of his account, was granted 24 hours of access and then was locked out again.

60. During its communications with Plaintiff Massery, Coinbase asked him for a copy of his passport and photo ID, something that Coinbase had never before requested of Plaintiff Massery. Coinbase claimed that the third-party hacker had used two-factor identification, but this was not possible because Plaintiff Massery received no such two-factor identification request from Coinbase for access to the account.

61. Coinbase never credited or provisionally credited Plaintiff Massery's stolen funds.

62. In short, Coinbase permitted, or failed to prevent, Plaintiff's and Class Members' Coinbase wallet accounts to be accessed by unauthorized third-party entities or linked to by third parties that had defrauded Plaintiff and Class Members. In those instances, the third parties had engaged in repeated activities across multiple Coinbase wallet account holders utilizing the functionality of their wallet accounts to steal Plaintiff's and Class Members' funds and cryptocurrency assets. Coinbase knew or should have known that the third-party entities were fraudulent because Coinbase knew the web addresses used to link to those entities through the Coinbase wallets and could have run basic scans and account monitoring to identity potential threats,

warn account holders and prevent access to such third-party sites through the wallet account functionality.

63. With proper monitoring of accounts for fraud, all of these transactions involving Plaintiff should have been flagged as suspicious.

64. Coinbase neither identified, prevented nor blocked those links, and did not provide any warning to Plaintiff or Class Members of the risks associated with those specific entities or links to their website address.

65. As a result of Defendants' acts and inaction, Plaintiff and the similarly situated putative class members they seek to represent have suffered injury in fact and lost money or property when their funds and cryptocurrency were stolen. Plaintiff and Class Members have all had assets stolen from their Coinbase wallet accounts and have been denied access to their accounts by Coinbase after reporting fraudulent transactions in their accounts.

66. To make matters worse, Coinbase received transaction fees of at least $3 from Plaintiff and Class Members for each fraudulent transfer and for each funding transaction Plaintiff and Class Members made to fund their accounts enabling such fraudulent transfers.

67. As a result, Plaintiff and Class Members have been further damaged by the transaction fees they paid to fund their Coinbase accounts with currency or crypto currency and to complete the fraudulent transactions resulting in the theft of their funds and assets.

CLASS ALLEGATIONS

68. This action is brought and may properly proceed as a class action pursuant to the provisions of Federal Rule of Civil Procedure 23.

69. Plaintiff seeks certification of a Class which is composed of and defined as follows:

> All current and former individual European Union Coinbase wallet account holders at any time on or after the day four years prior to the date on which this Complaint is filed, who transacted or maintained funds and/or cryptocurrency in their Coinbase wallet accounts, and who had such funds and/or cryptocurrency stolen as a result of Defendants' actions and/or failure to act to implement adequate security measures to protect account holder assets.

70. Excluded from the Class are Defendants' officers and directors, current or former employees, as well as their immediate family members, as well as any judge, justice, or judicial

officer presiding over this matter and members of their immediate families and judicial staff.

71. The members of the Class for whose benefit this action is brought are so numerous that joinder of all members is impracticable.

72. There are questions of law and fact common to the members of the Class that predominate over questions affecting only individuals. These common questions include, but are not limited to:

a. Whether Defendants owed duties to Plaintiff and the Class, the scope of those duties, and whether Defendants breached those duties;

b. Whether Defendants' conduct was unfair, unlawful or fraudulent;

c. Whether Defendants engaged in deceptive conduct;

d. Whether Plaintiff and the Class are entitled to damages as a result of Defendants' wrongful conduct; and

e. Whether injunctive relief is appropriate.

73. Plaintiff's claims are typical of the claims of the members of the Class which they seek to represent. All such claims arise out of the same policies, practices, procedures and other actions by Defendants, and the same or similar documents used by Defendants in their dealings with Plaintiff and Class Members.

74. Plaintiff has no interests antagonistic to those of the Class.

75. The Class, of which Plaintiff is a member, is readily identifiable.

76. Plaintiff will fairly and adequately protect the interests of the Class and have retained competent counsel experienced in the prosecution of consumer litigation. Class Counsel has investigated and identified potential claims in the action. Class Counsel has extensive experience in handling class actions, other complex litigation, and claims of consumers.

77. A class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all members is impracticable. While the economic damages suffered by the individual members of the Class are significant, the amount is modest compared to the expense and burden of individual litigation.

78. The questions of law or fact common to the members of the Class predominate over any questions affecting only individual members.

79. The prosecution of separate actions by individual members of the Class would run the risk of inconsistent or varying adjudications, which would establish incompatible standards of conduct for the Defendants in this action, or the prosecution of separate actions by individual members of the Class would create the risk that adjudications with respect to individual members of the Class would as a practical matter be dispositive of the interests of the other members not parties to the adjudications, or substantially impair or impede their ability to protect their interests. Prosecution as a class action will eliminate the possibility of repetitious litigation.

80. Defendants have acted, or refused to act, on grounds generally applicable to Plaintiff and Class Members, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Class as a whole.

81. A class action will cause an orderly and expeditious administration of the claims of the Class, and will foster economies of time, effort and expense.

82. Plaintiff does not anticipate any difficulty in the management of this litigation.

CAUSES OF ACTION

FIRST CAUSE OF ACTION

(Violation of the California Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq*.)

45. Plaintiff incorporates by reference and reallege each and every allegation contained above, as though fully set forth herein.

46. Defendants' user agreement, and associated Terms of Service, provides that "the laws of the State of California in the United States, without regard to its conflict of laws provisions," govern the Terms of Service and "any action related thereto."

47. Plaintiff, on behalf of themselves and the Class, brings this cause of action for violations of the "unlawful," "unfair," and "fraudulent" prongs of the Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq*. ("UCL").

48. Plaintiff and Defendants are "persons" within the meaning of the UCL. Bus. & Prof. Code § 17201.

49. The UCL prohibits unfair competition in the form of any unlawful, unfair, or fraudulent business acts or practices.

50. Section 17204 allows "any person who has suffered injury in fact and has lost money or property as a result of such unfair competition" to prosecute a civil action for violation of the UCL.

51. Coinbase's conduct was unlawful because it violated BSA and AML regulations applicable to money services business as set forth in 31 C.F.R. § 1022.210; the EFTA's error resolution provisions, 15 U.S.C. § 1693f; and because it violated the CLRA and the common law.

52. Plaintiff reserves the right to allege other violations of law, which constitute other unlawful business acts or practices. Such conduct is ongoing and continues to this date.

53. Defendants' acts and practices as alleged herein also constitute "unfair" business acts and practices within the meaning of the UCL. In the course of conducting business, Defendants have violated the UCL's proscription against unfair business practices by, among other things: (1) improperly and unreasonably representing that Plaintiff's and Class Members' wallet accounts, transactions within those accounts, and the assets held in those accounts were safe and secure; (2) failing to implement reasonable policies and procedures to preserve and safeguard customer funds as represented; (3) preventing Plaintiff and Class Members from accessing their accounts and funds, either for extended periods of time or permanently; (4) failing to timely respond to requests for support; (5) not compensating Plaintiff and Class Members for Defendants' wrongdoing and their losses; and/or (6) collecting transaction fees from Plaintiff and Class Members on fraud and theft related transactions.

54. Defendants' unfair business conduct is substantially injurious to consumers, offends legislatively-declared public policy as announced by the violations of the laws alleged, and is immoral, unethical, oppressive, and unscrupulous. The gravity of Defendants' wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendants' legitimate business interests other than engaging in the above-described wrongful conduct.

55. As a result of these actions and inaction, Defendants unfairly compete with other comparable companies in violation of Business and Professions Code sections 17000, *et seq*. and 17200, *et seq*. Due to these unlawful, unfair, and/or fraudulent business practices, Defendants have gained a competitive advantage over other comparable companies.

56. The UCL also prohibits any "fraudulent business act or practice." In the course of conducting business, Defendants committed "fraudulent business act[s] or practices" by among other things, failing to disclose to Plaintiff and other members of the Class that it would not adequately protect and secure Plaintiff's and Class Members' wallet accounts, the transactions within those accounts, and the assets held in those accounts; failing to disclose to Plaintiff and other members of the Class that it lacked adequate staffing to adequately protect Plaintiff's and Class Members' wallet accounts, the transactions within those accounts, and the assets held in those accounts; and failing to disclose to Plaintiff and Class Members that it could improperly and unreasonably restrict access to their wallets and accounts, and thereby prevent Plaintiff and other members of the Class from trading, withdrawing, or otherwise accessing their funds and cryptocurrency. These misrepresentations and omissions are contrary to what Coinbase represents is the entire supposed premise of its business – a safe, trusted, and easy-to-use platform to invest, store, spend, earn, and use crypto assets.

57. Plaintiff and Class Members have, in fact, been deceived as a result of their reliance on Defendants' material representations and omissions, which are described above.

58. The victims of Defendants' unlawful, unfair, and/or fraudulent business practices include, but are not limited to, Plaintiff and Class Members, competing cryptocurrency exchange platforms providing similar services as Defendants, and the general public. Plaintiff is informed and believe, and based thereon alleges, that Defendants performed the alleged acts with the intent of gaining an unfair competitive advantage and thereby injuring Plaintiff and Class Members, other competitors, and the general public.

59. Plaintiff's success in this action will enforce important rights affecting the public interest and public policy. In this regard, Plaintiff sues on behalf of himself and the public.

60. Business and Professions Code section 17203 provides that a court may make such orders or judgments as may be necessary to prevent the use or employment by any person of any practice which constitutes unfair competition. Injunctive relief is necessary and appropriate to prevent Defendants from repeating their unlawful, unfair, and fraudulent business acts and business practices alleged.

61. Business and Professions Code section 17203 provides that the Court may restore to any person in interest, any money or property that may have been acquired by means of such unfair competition.

62. Plaintiff and Class Members have suffered injury in fact and have lost money and property as a result of Defendants' unfair conduct. Plaintiff and Class Members are entitled to restitution pursuant to Business and Professions Code section 17203 for their account funds and cryptocurrency assets deposited into their Coinbase accounts that have been unlawfully withheld, the losses incurred as a result of Plaintiff and Class Members being unable to trade in their accounts, the money paid to Coinbase for the implementation of reasonable policies and procedures that would protect Plaintiff's and Class Members' accounts, and the fair value of other losses alleged herein, during the four-year period prior to the filing of this complaint. All remedies are cumulative pursuant to Business and Professions Code section 17205.

63. Plaintiff and Class Members request injunctive relief pursuant to Business and Professions Code section 17203 to enjoin Defendants from continuing the unfair/unlawful business practices alleged herein.

64. Plaintiff and Class Members have no adequate remedy at law.

65. Plaintiff herein takes upon enforcement of these laws and lawful claims. There is a financial burden involved in pursuing this action. The action is seeking to vindicate a public right, and it would be against the interests of justice to penalize Plaintiff by forcing Plaintiff to pay attorneys' fees from the recovery in this action. Attorneys' fees are appropriate, including pursuant to Code of Civil Procedure section 1021.5.

SECOND CAUSE OF ACTION

(Violations of the Consumers Legal Remedies Act, Cal. Civ. Code § 1750, *et seq*.)

66. Plaintiff incorporates by reference and realleges each and every allegation contained above, as though fully set forth herein.

67. Defendants' user agreement, and associated Terms of Service, provides that "the laws of the State of California in the United States, without regard to its conflict of laws provisions," govern the Terms of Service and "any action related thereto."

68. Defendants' acts and omissions as alleged herein were intended to deceive Plaintiff and Class Members, and have resulted in harm to Plaintiff and Class Members.

69. Defendants' actions as alleged herein violated, and continue to violate, California Civil Code section 1750, *et seq.* also known as the Consumer Legal Remedies Act ("CLRA") including section 1770(a)(5) for making representations that their services have characteristics, uses, or benefits which they do not, section 1770(a)(7) for making representations that their services are of a particular quality, which they are not, and section 1770(a)(9) for advertising services with intent not to sell them as advertised.

70. Pursuant to California Civil Code section 1782, attached herein as "**Exhibit A**" is a true and correct copy of Plaintiff's Notice of Violation of the California Consumer Legal Remedies Act (California Civil Code section 1750 *et seq*.) sent to Defendants on August 9, 2023. Once the time period set forth in California Civil Code section 1782(a) has expired after providing Notice and Demand to Defendant, Plaintiff will amend this cause of action to seek recovery of damages pursuant to California Civil Code section 1782(d).

71. Defendants' actions and omissions occurred in the County of San Francisco and Defendants maintains its principal place of business in the County of San Francisco. This action is brought in the California Northern District Court which presides over matters in the County of San Francisco. Attached hereto as "**Exhibit B**" is an affidavit setting forth facts showing this district is the proper place for trial pursuant to California Civil Code section 1780(d).

72. Pursuant to California Civil Code section 1780(a), Plaintiff and Class Members also are entitled to an order enjoining Defendants' wrongful acts alleged herein, an order awarding the

payment of costs and attorneys' fees pursuant to California Civil Code section 1780(e), and for such other relief that this Court deems just and proper.

THIRD CAUSE OF ACTION

(Breach of Contract and the Implied Covenant of Good Faith and Fair Dealing)

73. Plaintiff incorporates by reference and realleges each and every allegation contained above, as though fully set forth herein.

74. Plaintiff and Class Members each entered into a written contract, via their user agreement and associated Terms of Service, with Defendants upon their registration for a Coinbase wallet account. Plaintiff and Class Members were presented with the user agreement on a take-it-or-leave it basis and had no opportunity to negotiate any of the specific terms or provisions thereunder.

75. Every contract, including the user agreement, contains an implied duty of good faith and fair dealing. Defendants entered into and are bound by the user agreements with Plaintiff and Class Members, which are valid and enforceable contracts that contain an implied duty of good faith and fair dealing.

76. Defendants breached the user agreements and the implied covenant of good faith and fair dealing by, among other things, failing to discharge their obligations and provide the services they promised in exchange for the transaction fees they charged Plaintiff and Class Members for each transaction in their account and for the monies they earned on the funds within Plaintiff's and Class Members' accounts.

77. Specifically, Defendants breached the user agreements and the implied covenant of good faith and fair dealing by failing to protect the assets and transactions of Plaintiff and Class Members and failing to enable Plaintiff and Class Members to have immediate access to their accounts, the funds and cryptocurrency assets within those accounts, and to process only the respective customer's transactions within those accounts.

78. Defendants breached the user agreements and the implied covenant of good faith and fair dealing by failing to protect Plaintiff's and Class Members' accounts, their transactions relating to those accounts, and their funds and cryptocurrency assets within those accounts.

79. Defendants breached the user agreements and the implied covenant of good faith and fair dealing by failing to timely respond to and resolve Plaintiff's and Class Members' complaints regarding security threats, hacking, and technological issues that precluded Plaintiff's and Class Members' access to their accounts, account transactions and account funds and cryptocurrency assets.

80. Defendants breached the user agreements and the implied covenant of good faith and fair dealing by failing to timely notify Plaintiff and Class Members of any security threats, hacking, and technological issues that prevent Plaintiff's and Class Members' access to their accounts, account transactions and account funds and cryptocurrency assets.

81. Defendants breached the user agreements and the implied covenant of good faith and fair dealing by failing to meet their obligation of good faith and fair dealing to timely and properly resolve Plaintiff's and Class Members' complaints about their inability to access their accounts, account transactions and account funds and cryptocurrency assets.

82. Defendants breached the user agreements and the implied covenant of good faith and fair dealing by failing to meet their obligation to ensure that Plaintiff's and Class Members' could access their accounts, account transactions and account funds and cryptocurrency assets.

83. Defendants breached the user agreements and the implied covenant of good faith and fair dealing by failing to return Plaintiff's and Class Members' account funds and cryptocurrency assets.

84. As a result of Defendants' breach of their contractual duties, obligations and/or promises arising under the user agreement and the implied covenant of good faith and fair dealing, Plaintiff and Class Members were damaged by, including but not limited to, their payment of transaction fees, the loss of use of their accounts, the inability to access the funds and cryptocurrency assets in their accounts and the loss of value of those assets, all in an amount to be proven at trial.

85. In addition to Plaintiff's and Class Members' actual contract damages, Plaintiff and Class Members seek recovery of their attorney's fees, costs to the extent provided by the User Agreement and pre-judgment interest.

FOURTH CAUSE OF ACTION

(Unjust Enrichment)

86. Plaintiff incorporates by reference and realleges each and every allegation contained above, as though fully set forth herein.

87. Plaintiff and Class Members conferred a benefit upon Defendants by depositing their currency funds and cryptocurrency assets into their wallet accounts maintained by Defendants and maintained such assets in those accounts, and engaging in crypto transactions in those accounts, which enabled Defendants to profit from the investment and trading of such assets.

88. Plaintiff and Class Members conferred a benefit upon Defendants by paying fees to Defendants in order to conduct transactions in their accounts, maintain their accounts and have access to those accounts.

89. As a result of Defendants' actions and omissions alleged herein, Defendants have been unjustly enriched at the expense of Plaintiff and Class Members. Under principles of equity and good conscience, Defendants should not be permitted to retain the transaction fees paid by Plaintiff and Class Members or the assets held within Plaintiff's and Class Members' accounts.

90. Plaintiff and Class Members are entitled to restitution of, disgorgement of, and/or the imposition of a constructive trust upon all fee revenue, income, profits, and other benefits obtained by Defendants at the expense of Plaintiff and Class Members resulting from Defendants' actions and/or omissions alleged herein, all in an amount to be proven at trial. Plaintiff and Class Members also are entitled to attorney's fees, costs and prejudgment interest, along with any relief that this Court deems just and proper.

91. Plaintiff and the Class have no adequate remedy at law.

FIFTH CAUSE OF ACTION

(Conversion)

92. Plaintiff incorporates by reference and realleges each and every allegation contained above, as though fully set forth herein.

93. Defendants have asserted, and improperly maintained, dominion and control over Plaintiff's and Class Members' accounts, account funds and cryptocurrency assets by preventing

Plaintiff and Class Members to access their accounts and take possession of their account funds and cryptocurrency assets.

94. Defendants have allowed Plaintiff's and Class Members' funds and cryptocurrency assets to be depleted and Defendants have benefited thereby by improperly retaining such funds and cryptocurrency assets or by transaction fees paid by others that have taken Plaintiff's and Class Members' funds and cryptocurrency assets without their authorization.

95. Plaintiff and Class Members are entitled to restitution of, disgorgement of, and/or the imposition of a constructive trust upon all fee revenue, income, profits, and other benefits obtained by Defendants at the expense of Plaintiff and Class Members resulting from Defendants' actions and/or omissions alleged herein, all in an amount to be proven at trial. Plaintiff and Class Members also are entitled to attorney's fees, costs and prejudgment interest, along with any relief that this Court deems just and proper.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself, and all others similarly situated, respectfully prays for relief as follows:

A. An order certifying the Class for declaratory and injunctive relief and for money damages under Federal Rules of Civil Procedure Rule 23 and California Civil Code section 1781(a), appointing Plaintiff as Class Representative, and appointing their attorneys as Class Counsel;

B. A judgment for actual damages;

C. A judgment for compensatory damages;

D. A judgment for restitution;

E. A judgment for disgorgement of transaction fees, income and other profits;

F. A declaratory judgment that Defendants violated the UCL and CLRA;

G. A judgment for injunctive relief enjoining Defendants from engaging in future unlawful activities complained of herein, including violations of the UCL and CLRA;

H. An order that Defendants shall engage in corrective actions so that customer accounts, funds and cryptocurrency assets can be secured, accessed and transacted;

I. An accounting of all amounts that Defendants unjustly received, retained, and/or collected as a result of their unlawful acts and omissions;

J. Pre-judgment and post-judgment interest;

K. A judgment for reasonable attorney fees and costs of this suit, pursuant to contract, the UCL, California Civil Code Section 1780(e), California Civil Code section 1021.5, and any other applicable statute; and

L. A judgment for all such other and further relief as the Court deems equitable and just.

Respectfully submitted,

Dated: August 9, 2023

BLOOD HURST & O'REARDON, LLP
TIMOTHY G. BLOOD (149343)
PAULA R. BROWN (254142)
JAMES M. DAVIS (301636)

By: *s/ Timothy G. Blood*
TIMOTHY G. BLOOD

501 West Broadway, Suite 1490
San Diego, CA 92101
Tel: 619/338-1100
619/338-1101 (fax)
tblood@bholaw.com
pbrown@bholaw.com
jdavis@bholaw.com

EVANGELISTA WORLEY, LLC
James M. Evangelista (*pro hac vice forthcoming*)
500 Sugar Mill Road, Suite 245A
Atlanta, GA 30350
Tel: 404/205-8400
404/205-8395 (fax)
jim@ewlawllc.com

Attorneys for Plaintiff